Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Adventures in Computer Forensics

What exactly do forensic analysts do? How can this type of work help law enforcement or corporate security managers? If you want to solve a puzzle isn't it often best to have all the pieces? Computer forensics is one piece to the investigative puzzle. There must be some need to conduct this type of investigation. Security managers and law enforcement alike must have proper authorization before conducting this type of analysis on a computer. Security managers should get this in writing as part of their security policy. ...

Copyright SANS Institute
Author Retains Full Rights

AD

Adventures in Computer Forensics

By Diana J. Michaud
EWA, IIT

What exactly do forensic analysts do? How can this type of work help law enforcement or corporate security managers? If you want to solve a puzzle isn't it often best to have all the pieces? Computer forensics is one piece to the investigative puzzle. There must be some need to conduct this type of investigation. Security managers and law enforcement alike must have proper authorization before conducting this type of analysis on a computer. Security managers should get this in writing as part of their security policy. Check with your lawyers and be aware of privacy laws and how they apply even in the corporate setting. The privacy laws may go beyond a consent to search and consent to monitoring. We can often help piece together past events by looking at recovered files, internet cache, and slack space. Sometimes, just looking at what someone wanted to get rid of is a good place to start, other times you will need to dig a little deeper and look at areas of the hard disk that the normal user does not usually have access to. When these cases are tried in court, the defense will spend time trying to discredit the analyst. It is their job to create doubt in the procedures you have used to conduct your analysis, and possibly that it wasn't his client that put the information there. As the analyst it is your job to report what you found not to speculate, or follow down the path of doubt the defense tries to create. You must be able to stand up against some professional and personal scrutiny. Lawyers don't like to take cases that have "issues". Don't let your procedures be one of those issues. It is important for the analyst to be able to find the evidence on a computer and be able to articulate how you found the evidence. It is great to be able to retrieve evidence from a computer, but having an idea of how it works, how data is saved in various operating systems, and being able to describe this to someone else is crucial. Cases are often won on perception of the facts not just the facts. Others will need to understand what you are talking about, be it a criminal or civil case. I like to use the acronym PPAD. This stands for Preserve the data to ensure the data is not changed, Protect the evidence to ensure no one else has access to the evidence, Analyze the data using forensically sound techniques, and Document everything.

It will make you a better analyst to have a solid foundation in computer hardware and how operating systems work. It is a good idea to have an understanding of what a normal operating system looks like before you can begin to see the differences. Knowing about how drives are partitioned, how you can hide partitions, where the partition table may be found on different operating systems, what the master boot record is and what a normal one looks like. You should know what drive geometry is and how this can be used. I would recommend formalized training to get started in this field. Training can bring a lot of credibility to this field, as well as, allow you the time to test different tools. Allowing yourself to hide files, delete directories and recover them can be valuable time spent familiarizing yourself with how different forensic tools and different operating systems work. This allows you to get some experience in how things should look so the analyst can start seeing what should or should not be there. We

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

know files can be renamed. You really can't make a judgment call on whether the file is what the file extension says it is. Be familiar with file headers and the extensions that may be associated with that particular file. It is also possible that the user may try to hide files by renaming them to look like regular operating system files; so being familiar with what should be there and what it looks like will help you be a better analyst.

It is essential to have some written standard operating procedures (SOP) in which you conduct yourself every time. These procedures will allow you to be absolutely sure you have not contaminated the case with your own data or data from a previous case. The initial response to an incident is just as important that the analysis. What happens first can greatly impact the laboratory analysis. Unqualified individuals should not be allowed near the scene, nor should anyone be allowed to remove anything from the scene until qualified and trained security personnel arrive. The integrity of the process, as well as, the integrity of the data is paramount to any analysis. Having written documentation about how you will seize the computer, protect the evidence, conduct the analysis and report what you found is great to lean back on. This is where I use the acronym PPAD. Preserve, Protect, Analyze, Document. I try to keep it simple and we never have enough acronyms in this business. Under each of these topics you can have procedures in writing. You can then definitively say you conducted the analysis this way because that is the way I always conduct myself. Also keep a log and proper documentation to support that. You should clean up after previous cases and prepare your area for the new one. As part of your SOP, there should be policy on the way you have your analysis workstation configured. For example, prior to starting a case I prepare my workstation by updating the anti-virus definitions, wipe the drive I use to restore the working copy to, and organize the area where I will save data pertinent to the investigation. I know we all seek the truth and you wont find it by accidentally looking at the previous case and confusing it with the new one. Create a folder to save the new case information to and try to keep the files labeled so they make sense to you. For example, if I find data on the physical level in Cluster 19985, I would save the data c19985.txt and so on. Different analysts organize their cases differently. Find a way that works for you. You will want to have any area to work in that limits access by others so there will be no question in your mind whether the data was compromised. The analyst's machine should be a stand-alone system and not be networked. Not having your computer networked will make you to be more confident that there was no access to the machine through your locked door.

The next part of conducting a forensically sound computer investigation would be to safeguard your evidence and have a chain of custody. While seizing a computer remember not to allow the user any further access to the computer and then approach carefully. No one else should have access to the data. This way you are sure that the data has not been tampered with. As soon as you approach the scene start a chronological log of the steps you take. Your notes should entail who you talked to, what the scene looked like when you arrived, and any other observations made. Make notes about the computer including a date, time and description of the computer. This may not seem important until you realize later when you need to correlate other types of logs with the computer you are analyzing. If you are analyzing a server you will want to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

check the event logs as well. Some logs have a default GMT time and unless the system administrator reset the logs to show the actual time you will need to do some math to correlate what the logs say and what actually happened. Don't change anything-just document the time difference. The user can easily change the time on the computer. Be aware of this and how time may or may not match up with the chronological events in the case. For example the files in question may have been accessed on a Saturday and the user was not at work then. In this case you can only document this and hopefully your case has more evidence than just date and times. Open the computer up and see if there is more than one hard drive, make notes of what peripherals are attached, including the serial number of the hard drive for future correlation. It is a good idea to label and photograph everything so you can put it back together later and remember just how the user had it set up. If you are not taking the entire computer and related material with you it is imperative that you get all the information you need on site because you may not be allowed to come back. At this point you might take a look around the area for password information (yes some still keep them on a yellow sticky). If you find yourself having to break through passwords during analysis you can consider using several tools on the market or just asking the user. You never know, the user just might feel like cooperating. Also look for peripheral storage devices like zip disks, floppies, and image disks. Evidence might come in a very small package, especially with the media that come with digital cameras. It is also possible that even if the computer looks like a standalone system that there may be a USB port or PCMCIA slot that you can plug in a network device and configure networking even though it looks like a standalone system when you get to the scene. Ask the systems administrator if this user was supposed to have access from home and ask for the VPN logs to check for last access times to the host.

There is great debate in the forensic community over the point of whether to unplug or not to unplug a system. One of the most difficult decisions you will have to make, as a first responder is how to power down the machine. The operating system involved will be the key in this decision. If it is a compromise or intrusion investigation you may want to check if there are existing processes running in memory, file systems mounted remotely via the network and any other suspicious connections to that host and what ports are being utilized. The user may have chose to save some files to a server somewhere or another users system in an effort not to implicate him or herself. Also if the system is on, and there is evidence on the screen, you can photograph the screen or print screen and save to a floppy prior to shutting down. You may choose to check some of the processes on site, check the host logs, look for core files immediately in case someone is trying to erase their tracks. If you unplug the machine and there are additional leads to your investigation via the network, you have lost those leads and failed to see the bigger picture of your investigation. You may want to do a netstat command and redirect the output to a file on a floppy to capture the current connections. It is also possible, if it is hooked to a network, that remote access may allow someone to attempt to dispose of possible evidence remotely. You may want to pull the plug, depending on the type of case, because if you shut down gracefully there may be programs that will execute on shutdown and dispose of evidence by running a wipe utility, for example. If you feel you need to pull the plug to preserve evidence, pull

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

it on a Windows system. I would not recommend pulling the plug in a Unix environment unless you have had experience rebuilding an inode table. You don't want to destroy the evidence on the original right from the start, but again if you feel you have no other choice you might have to pull the plug from the wall. In a case where you need to do an immediate shutdown, halt the system immediately, pull the network connection and begin using an image utility for that operating system. You will have to make a judgment call at this point just be sure to document everything so you can articulate later why you did what did. If the machine is off leave it off. If it is a Windows system boot the computer with a controlled boot disk. A controlled boot disk is one that controls the initial booting process so the operating system does not start writing to the disk. Some operating systems begin writing to the drive immediately and can change access times and possibly write over data that may be pertinent to your case. There is always a risk, but if you use a control boot disk first, create a bit level image and then create another copy and do your analysis on the working copy, you are less likely to damage the evidence. As soon as you begin the booting process, go in the BIOS and look at the how the user has set the drive geometry. There may be several settings to choose from including, logical block addressing and normal depending on the size of the drive. You will want your image to mirror the user settings so document what you find in the BIOS. You may need to set the BIOS to auto so it can detect the drive you are imaging to. Prior to doing analysis on the working copy you must write protect the media. This also allows for some confidence in the fact that you did not contaminate the data in any way. There are various software tools that do this for hard drives. For floppies you can test the write protect ability of the machine by using a disk that is NOT associated with the case, physically write protect it and try to write to it. If you get an error message then you know the floppy device is working properly and you can proceed with your analysis. A bit level image is the preferred method of imaging. The bit level image allows you to get an image of the media including the slack space and every 0 and 1 on the disk. Slack space is the space between the end of the file and the end of the cluster. Data can be retrieved from this area if it was used before and overwritten by the new file that is smaller. You may also find data in this area if someone uses an editor and physically accesses the cluster and written to this area in an attempt to hide data not recognized by the operating system's directory.

There are many tools and utilities you can use to make a bit level image. It is best to get some tools and test them in a controlled environment to make sure you are getting the entire physical parameters of the media. At this time you can begin your imaging with your imaging utility. You should use a brand new hard drive to image to or a hard drive that you have run a wipe utility on and verified it is clean. You can verify this by using a disk-editing tool and looking at random physical sectors of the media and ensuring that there is no data on the media prior to obtaining your image of the evidence. After you have imaged the data you should lock up the original and do the analysis on the imaged copy. There are various tools you can use to look at the system area and the data area on the media. There are times where you may need to go in the machine on a logical level, which may change dates and times. You can always go back and reimage the original; however only if it is truly necessary. I conduct most of my analysis on the physical level and at the end of the analysis go into the logical level

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

and look at images and other files not easily viewed at the command prompt like text files. You should keep a log of your procedures. You can't always rely on your memory after a year, when it makes it to court, on how you conducted the analysis. It seems the defense in these cases would prefer to poke more holes in the procedures you use, than the fact that the evidence found was on the computer, so make sure you document properly. Be able to articulate in court that you booted into the computer at the end of your analysis and doing so changed the date and time, but that operation doesn't create pictures or evidence. Just opening a file alters the time and date it was last accessed. This can be extremely important to the defense so be aware of this and conduct your analysis on the physical level or with forensic tools that do not alter this information. If the defense would like to see the original dates and times you can also create another working copy and do a DIR command and redirect to a file and capture the dates and times associated with the files.

Forensic analysis is conducted on two levels. The first is the physical level where you would look at individual clusters and sectors for information. I prefer to conduct the initial phase of analysis on this level. This initial search should include looking at the master file table, or file allocation table depending on the operating system. This is a section that is generally referred to as the system area and not usually accessed by the user. Analysis should cover the system area, as well as, the data area since even though it is not normally accessed it is a place where data can be placed. I like to do most of my investigation using tools on the physical level. I run string searches in this mode to look through the entire hard drive for keywords pertaining to the case. I also run utilities on this level to search for erased files and recover them. This is also the level where you can look at file slack and find information for your case. You cannot see this area by booting into the system. You can find a lot of information just looking for what the user wanted to get rid of. The second is a logical level where you might boot into the machine and look for evidence as the user sees the computer. On the logical level you can view graphics, which look like a bunch of encryption when looking at it in hexadecimal mode. You can set the browser to work offline and view the users cache and possibly find leads to other information, like alias email accounts other than the one configured for the user to use. You can also save files out to a floppy on the physical level and view from another drive and never boot into the evidence.

There are various password cracking, imaging, and investigative tools on the market. It is far more important to personally test and evaluate your tools. If some organization has written about how great the tool is, test it yourself. Then you can say, I know it works because I have tested it not just because you have read something about it. Last, keep up on what is new in this field. Subscribe to forensic newsgroups and magazines. It is better to be aware of bugs in your tools than be told about them in court. I have tried to focus my topic on procedures and methods and not just the latest and greatest tool. By staying with the methods mentioned in this paper I hope you can go forth and conduct thorough, unbiased, forensically sound examinations.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Farmer, Dan and Venema, Wietse. Forensic Computer Analysis: An Introduction
http://www.ddj.com/articles/2000/0009/0009f/0009f.htm (30 July 2001)

"Basic Steps in Forensic Analysis of Unix Systems."
http://staff.washington.edu/dittrich/misc/forensics (1 AUG 2001)

Armstrong, Illena. "Computer Forensics."
http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html (4 AUG 2001)

Armstrong, Illena. "Computer Forensics: Tracking Down the Clues". SC Magazine April 2000, Vol 12, No 4.

Holley, James. "Getting the Hard Facts." SC Magazine (3 AUG 2001)

Other associated groups and information:

The National Cybercrime Training Partnership http://www.nctp.org

The Regional Computer Forensic Group (RCFG) http://www.rcfg.org

The International Association of Computer Investigative Specialist
http://www.cops.org

http://www.fish.com Just a good security site and some related forensic material.

© SANS Institute 2001, Author retains full rights

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced